

P1 1171555

REC'D 24 MAY 2004

WIPO PCT

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

May 19, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: 60/458,314

FILING DATE: March 28, 2003

RELATED PCT APPLICATION NUMBER: PCT/US04/09781



By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS


P. R. GRANT
Certifying Officer

**PRIORITY
DOCUMENT**

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

BEST AVAILABLE COPY

03-31-03 03/28/03 PTO/SB/16 (10-01)
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Express Mail Label No.

EL692649056US

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
G. Eric Engstrom Peter	Engstrom Zatloukal	Kirkland, Washington Kirkland, Washington

☐ Additional inventors are being named on the _____ separately numbered sheets attached hereto

TITLE OF THE INVENTION (500 characters max)

A Wireless Mobile Phone With Authenticated Mode of Operation Including Finger Print Based Authentication

Direct all correspondence to:

CORRESPONDENCE ADDRESS

☒ Customer Number

000025943

Type Customer Number here

Place Customer Number
Bar Code Label here

OR

☐ Firm or
Individual Name

Address

Address

City

State

ZIP

Country

Telephone

Fax

ENCLOSED APPLICATION PARTS (check all that apply)

☒ Specification Number of Pages

17

☐ CD(s), Number

☒ Drawing(s) Number of Sheets

9

☒ Other (specify)

Return receipt postcard

☐ Application Data Sheet. See 37 CFR 1.76

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. See 37 CFR 1.27.

☒ A check or money order is enclosed to cover the filing fees

☒ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number:

500393

☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE
AMOUNT (\$)

\$160.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE

Robert T. Watt

TYPED or PRINTED NAME Robert T. Watt

TELEPHONE 503-222-9981

Date 03/28/2003

REGISTRATION NO.
(if appropriate)
Docket Number:

45,890

109909-132415

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

PROVISIONAL APPLICATION FOR UNITED STATES PATENT

FOR

**A WIRELESS MOBILE PHONE WITH AUTHENTICATED MODE OF
OPERATION INCLUDING FINGER PRINT BASED
AUTHENTICATION**

Inventors
G. Eric Engstrom
Peter Zatloukal

Prepared by: Schwabe, Williamson & Wyatt, PC
Pacwest Center
1211 SW Fifth Ave., Ste 1600-1900
Portland, Oregon 97204

Attorney Docket No.: 109909-132415
IPG No: P053Z

Express Mail Label No. EL692649056US

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

A WIRELESS MOBILE PHONE WITH AUTHENTICATED MODE OF OPERATION INCLUDNIG FINGER PRINT BASED AUTHENTICATION

FIELD OF THE INVENTION

5 The present invention relates to the field of wireless mobile phones. More specifically, the present invention is related to a wireless mobile phone having an authenticated mode of operation available only to an authenticated user, in particular, a user authenticated via the user's finger print.

BACKGROUND OF THE INVENTION

10 Advances in microprocessor and telecommunication technology have led to wide spread deployment and adoption of mobile devices, such as wireless mobile phones. For wireless mobile phones, in addition to wireless telephony, the late models are often equipped with advanced capabilities, such as calendar,
15 address book, access to the World Wide Web (WWW), emails, and so forth.

 Much of these functionalities are designed to increase the productivity of business users. As a result, it is not surprising that business users constitute a major user segment of wireless mobile phones, especially for the high-end function rich models. Increasingly, more business data, such as business
20 contact information, business plans, sales/marketing strategies, financial reports, and so forth, are being stored on wireless mobile phones.

 However, unlike personal computers or other computing devices, where user authentication, through e.g. user log-in, are routinely provided with virtually all operating systems, few if any operating systems of wireless mobile phones
25 provide means to authenticate users. As a result, under the prior art, wireless

mobile phones are at risk of unauthorized usage, as well as data being compromised by unauthorized accesses.

Thus, it will be desirable if protection against unauthorized access of user data and/or usage of wireless mobile phones can be provided.

5

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be described by way of exemplary embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

10

Figure 1 illustrates a front view of a wireless mobile phone incorporated with the teachings of the present invention, in accordance with one embodiment;

15

Figures 2a-2b illustrate a top view and a side view of the power switch of **Fig. 1**, having an integrated finger print reader, in accordance with one embodiment;

Figures 3a-3b illustrate two architectural views of the wireless mobile phone of **Fig. 1**, in accordance with one embodiment;

Figures 4a-4b illustrate the operational flow of the relevant aspects of the operating logic of **Fig. 3b**, in accordance with one embodiment;

20

Figure 5 illustrates a front view of another wireless mobile phone incorporated with the teachings of the present invention, in accordance with an alternate embodiment;

25

Figures 6a-6b illustrate two perspective views of another wireless mobile phone incorporated with the teachings of the present invention, in accordance with yet another embodiment;

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

Figures 7a-7b illustrate a front view and a side view of another wireless mobile incorporated with another aspect of the teachings of the present invention, in accordance with yet another embodiment; and

Figures 8a-8b illustrate a front view and a back view of the identity card of

5 **Fig. 7b** in further detail, in accordance with one embodiment.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

The present invention includes a wireless mobile phone having an
10 authenticated mode of operation, available only to an authenticated user, in particular, a user authenticated by the user's finger print.

Parts of the description will be presented in terms commonly employed by those skilled in the art to convey the substance of their work to others skilled in the art. The term "wireless mobile phone" as used herein (in the specification
15 and in the claims) refers to the class of telephone devices equipped to enable a user to make and receive calls wirelessly, notwithstanding the user's movement, as long as the user is within the communication reach of a service or base station of a wireless network service provider. Unless specifically excluded, the term "wireless mobile phone" is to include the analog subclass as well as the digital
20 subclass (of all signaling protocols).

In the following description, various aspects of the present invention will be described. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention. For purposes of explanation, specific numbers, materials and
25 configurations are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

present invention may be practiced without the specific details. In other instances, well-known features are omitted or simplified in order not to obscure the present invention.

Various operations will be described as multiple discrete steps in turn, in a manner that is most helpful in understanding the present invention, however, the order of description should not be construed as to imply that these operations are necessarily order dependent. In particular, these operations need not be performed in the order of presentation.

The phrase "in one embodiment" is used repeatedly. The phrase generally does not refer to the same embodiment, however, it may. The terms "comprising", "having" and "including" are synonymous, unless the context dictates otherwise.

Referring now to **Figures 1 and 3a-3b**, wherein a front view and two architecture (internal component) views of a wireless mobile phone of the present invention, in accordance with one embodiment, are shown. As illustrated, wireless mobile phone **100** of the present invention (hereinafter, simply phone **100**) is advantageously provided with operating logic **240** equipped in particular with security function **242**, to operate phone **100** in at least an unauthenticated mode of operation and an authenticated mode of operation.

While operating in the unauthenticated mode of operation, i.e. without having the user authenticated, operating logic **240** makes available only a limited or reduced set of functions, whereas under the authenticated mode of operation, i.e. having the user authenticated, operating logic **240** makes available a more expanded or the entire set of functions.

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

The exact constitution of the limited/reduced set of functions and the expanded/full set of functions is application dependent, which may vary from embodiments to embodiments. In one embodiment, the limited/reduced set of functions include only the ability to make an emergency call, such as a 911 call,
5 otherwise, no other functions, including but not limited to making other calls, accessing calendar, email, text messaging, viewing and/or storing documents, and so forth, are permitted. These other functions are available only under the authenticated mode.

In another embodiment, the limited/reduced set of functions may
10 effectively be a null function set, excluding even the ability to make an emergency call, except for notification of the unauthenticated status of the user, and perhaps, inviting the user to authenticate himself/herself, by e.g. providing a finger print input.

In various embodiments, in addition to the above described
15 unauthenticated and authenticated modes of operation, operating logic 240 further supports a provisioning mode of operation, under which phone 100 is initially provisioned. Under the initial provisioning mode, conventional provisioning, such as configuring phone 100 for a particular wireless carrier, a particular subscriber and so forth, may be performed. Entry into the initial
20 provisioning mode may be effectuated in any one of a number of conventional approaches.

Continue to refer to **Figures 1 and 3a-3b**, for the illustrated embodiment, phone 100 is further advantageously equipped with finger print reader 232 to facilitate a user to input his/her finger print, and security function 242 is equipped
25 to authenticate the user by the user's inputted finger print. In other words, operating logic 240 operates phone 100 in the authenticated mode, and makes

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

available the expanded/full set of functionalities, only if the user has been authenticated by his/her finger print, otherwise, phone 100 is operated in the unauthenticated mode with only a limited/reduced set of functionalities (except in the initial provisioning mode).

5 For the embodiment, operating logic 240, more specifically, security function 242, also supports the provision of a finger print, and its saving in the form of an image, for use as a reference to authenticate an inputted finger print for authentication of a user, and operation of phone 100 in the authenticated mode. In various embodiments, the saving of the reference finger print image is
10 also supported under a special configuration mode, while operating in the authenticated mode. Entry into the configuration mode (while operating in the authenticated mode) may also be effectuated in any one of a number of conventional means.

 Further, for the illustrated embodiment, finger print reader 232 is
15 advantageously integrated with power on/off button 122, to enable a user's finger print to be inputted seamlessly as part of the power-on process.

 Moreover, for the illustrated embodiment, power on/off button 122 (integrated with finger print reader 232) is disposed at the top end surface of body 116 of phone 100. As will be described in more detail below, referencing
20 Figs. 5 and 6a-6b in particular, power on/off button 122 (integrated with finger print reader 232) may be disposed on other surfaces of the body of a wireless mobile phone.

 Referring now also to Figures 2a-2b, wherein a top view and a side view of power on/off button 122 with integrated finger print reader 232 is illustrated in
25 further detail, in accordance with one embodiment. As illustrated, for the embodiment, power on/off button 122 includes transparent body 124 (which

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

transparency is represented by the hash lines) having flanges **126**, which undersides include contacts **142**. Contacts **142** are employed to close/open switch circuit **228**, as power on/off button **122** is moved from a rest position to a depressed position. When closed, switch circuit **228** allows power from power supply **222** to be provided to from finger print reader **232** and other components **202-212** of phone **100**. When open, switch circuit **228** cutoffs power of power supply from finger print reader **232** and other components **202-212** of phone **100**. Power on/off button **122** also includes a counterforce exerting means (not shown), such as a spring like assembly, to exert a counterforce to restore power on/off position **122** from the depressed position to its rest position.

For the embodiment, finger print reader **232** includes light source **234** and sensors **236**. Light source **234** is employed to emit light, and sensors **236** are employed to sense the emitted light (passing through transparent body **124** of power on/off button **122**) and reflected off finger **150** of the user (back through transparent body **124** of power on/off button **122**). In one embodiment, light source **234** comprises one or more light emitting diodes (LED), and sensors **236** comprise an array of micro photo sensors.

Sensors **236** output signals responsive to the reflected light sensed. The signals in turn are processed by DSP **204** into an image, more specifically, an input finger print image. Security function **242**, executed by processor **202**, in turn compares the input finger print image against the reference finger print image to authenticate the user.

In alternate embodiments, non-optical finger print readers, such as capacitance based finger printer readers may be employed instead. For these embodiments, sensors **236** output signals responsive to the electrical interactions between the embedded capacitors and the user's finger, which vary according to

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

the print contour. The signals output by sensors 236 may be processed into a finger print data structure and/or image. In yet other embodiments, other non-capacitance based, non-optical finger print readers may be employed instead.

Referring again to Fig. 1 and 3a-3b, additionally, phone 100 include
5 conventional wireless telephony elements, including audio communication elements, such as ear speaker 112 and microphone 114, and non-audio communication elements, such as input key pad 102 having a number of alphanumeric input keys and display 108. Further, the non-audio input elements may further include scroll button 105, selection buttons 106, and "talk" and "end
10 talk" buttons 104. These elements are disposed on various external surfaces of body 116.

Externally, phone 100 may also include antenna 110. Keys of key pad 102 may be surrounded by, or otherwise include illuminable light emitting diodes (LED) in their backgrounds. For the purpose of the present specification, the
15 terms "button" and "key" may be considered synonymous, unless the context clearly indicates otherwise.

Internally, in addition to processor 202 and DSP 204, phone 100 also includes non-volatile memory 206, general purpose input/output (GPIO) interface 208, and transmit/receive (TX/RX) 212, coupled to each other, processor 202
20 and DSP 204, via bus 214, and disposed on a circuit board 220.

Except for novel manner that many of these elements, such as processor 202, DSP 204 and so forth, are used in support of making the expanded/full set of functionalities available only to an authenticated user, the enumerated elements otherwise perform their conventional functions known in the art.

25 Non-volatile memory 206 is employed to store programming instructions and optionally, working data, including operating logic 240 and its security

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

function 242. Working data may include callee/messaging party or parties (e.g. their phone numbers or IP addresses) with whom user may communicate. Working data may include the reference and input finger print images of the user.

Processor 202, assisted by DSP 204, is employed to operate phone 100,
5 executing operating logic 240, including security function 242.

Keys of key pad 102 may be employed to enter alphanumeric data, including entering a sequence of alphanumeric data for the phone number or address of a "callee". Selected sequence of the keys (such as "**#") may also be employed to denote a user instruction to return to the unauthenticated mode of
10 operation, if entered while operating in the authenticated mode of operation, or to return to the authenticated mode of operation, if entered while operating in the unauthenticated mode of operation (provided the user is authenticated).

Scroll key 105 and companion selection keys 106 may be employed to scroll and select various options or list items of various menu options or selection
15 lists, including scrolling and selecting list items presented for user interactions to verify the user's wellness. For the embodiment, scroll key 105 may be selected in one of two positions, an "up" position or a "down" position for scrolling a selection list in an "up" direction and a "down" direction respectively. Similarly, scroll and selection keys 105/106 may also be employed to select a menu item to
20 convey a user instruction to return to the unauthenticated mode, if the selection is made while operating in the authenticated mode, or to return to the authenticated mode, if the selection is made while operating in the unauthenticated mode (provided the user is authenticated).

GPIO 208 may be employed to generate input signals, such as a
25 corresponding "alphanumeric" signal in response to a user selection of one of the keys of key pad 102, a "scroll" signal" (or more specifically, a "scroll up" or a

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

"scroll down" signals) in response to a user selection of scroll key 105, a "selection" signal in response to a user selection of select button 106, and so forth.

TX/RX 212 may be employed to transmit and receive communication signals for a call and/or a text message. TX/RX 212 may be a radio frequency transceiver, and support one or more of any of the known signaling protocols, including but are not limited to CDMA, TDMA, GSM, and so forth.

The constitutions of these elements are known, and will not be further described.

As to operating logic 240, including security function 242, it may be implemented in the assembly or machine instructions of processor 202, or a high level language that can be compiled into these assembly or machine languages.

Accordingly, except for the enhancements provided, phone 100 otherwise represents a broad range of wireless mobile phones, including both the analog as well as the digital types (of all signaling protocols), substantially rectangular uni-body as illustrated, or curved uni-body, as well as multi-portions, such as "flip phones" to be illustrated later.

Figure 4 illustrates the operational flow of the relevant aspects of operating logic 240, in accordance with one embodiment. As illustrated, on start up/reset (such as depression of power on/off button 122 by a user), operating logic 240 enables phone 100 to operate in the earlier described unauthenticated mode, making available only a limited/reduced set of functionalities, block 402. Thereafter, operating logic 240 waits for additional user input, block 404.

Recall from earlier description, on closure of switch circuit 228, power is provided to finger print reader 232 and other components 102-212 of phone 100.

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

Thus, if a user continues to keep his/her finger on power on/off switch, even after closing switch circuit **228** and powering on phone **100**, integrated finger print reader **232**, supported by DSP **204**, enables a finger print image to be seamlessly inputted for user authentication.

5 Accordingly, on receipt of inputs, operating logic **240** determines if the input is finger print input provided via finger print reader **232**, block **406**. In various embodiments, processor **202** may be notified (e.g. interrupted) by DSP **204** upon completion by DSP **204** in generating an input finger image.

10 If the user input is a finger print image, operating logic **240** (or more specifically, security function **242**) determines if phone **100** is operating in the unauthenticated mode, within the configuration mode of the authenticated mode, or the initial provisioning mode, block **407**.

15 If phone **100** is determined to be operating in either, the configuration mode within the authenticated mode, or the initial provisioning mode, operating logic **240** (or more specifically, security function **242**) saves the inputted finger print image as a reference finger print image, block **408**.

20 If phone **100** is determined to be operating in the unauthenticated mode, operating logic **240** (or more specifically, security function **242**) initiates the finger print based authentication process, authenticating the user by comparing the received input finger print image, against the previously saved reference finger print image, block **409**.

25 If the inputted finger print image does not substantially match the previously saved reference finger print image, block **410**, operating logic **240** (or more specifically, security function **242**) reports the authentication failure, block **412**, and continues to operate phone **100** in the unauthenticated mode at block **404**.

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

However, if the inputted finger print image substantially matches the previously saved reference finger print image, block 410, operating logic 240 (or more specifically, security function 242) enables phone 100 to operate in the authenticated mode, block 414. Thereafter, operating logic 240 continues
5 operation at block 404.

The precision level at which an inputted finger print image is to be considered substantially matching with a reference finger print image is application dependent. Preferably, different user selectable precision levels are offered. As with other user selectable options, the selection may be facilitated in
10 any one of a number of known user selection techniques.

Back at block 408, if the input is determined not to be finger print input, operating logic 240 determines if the input is a user instruction to return to the unauthenticated mode of operation (e.g. a user selecting or inputting such command using alphanumeric keys 102 and/or scroll/select keys 105 and 106
15 while operating in an authenticated mode of operation), block 416.

If the input is determined to be a user instruction to return to the unauthenticated mode of operation, operating logic 240 (or more specifically, security function 242) returns phone 100 to operate in the unauthenticated mode, block 418. Thereafter, operating logic 240 continues operation at block 404.

20 In one embodiment, before exiting to the unauthenticated mode, operating logic 240 (or more specifically, security function 242) causes a user selectable "resume" (i.e. re-authentication) option to be rendered on display 108. Selection of the option is processed as if phone 100 is being powered on or reset. That is, operating logic 240 causes a finger print of the user to be read and inputted.

25 If the input is determined to be other user inputs, operating logic 240 handles the other user inputs in an application dependent manner, block 420. In

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

particular, if the input is a user instruction to return to the authenticated mode of operation, operating logic 240 continues operation at block 404, and awaits for finger print input. If the input is other conventional inputs, the inputs are processed as in the prior art. Thereafter, operating logic 240 continues operation
5 at block 404.

Figure 5 illustrates another embodiment of the wireless mobile phone of the present invention. More specifically, Fig. 5 illustrates a front view of the alternate embodiment. The alternate embodiment is substantially that of the
10 embodiment of Fig. 1, except that phone 100 is substantially rectangular in shape, whereas phone 500 has a curved shape. Also, power on-off button 522 with integrated finger print reader is disposed at a side surface of body 516 of phone 500 instead.

15. Figures 6a-6b illustrate yet another embodiment of the wireless mobile phone of the present invention. More specifically, Fig. 6a-6b illustrate two perspective views of the embodiment. The embodiment is also substantially that of the embodiments of Figs. 1 and 5, except that phone 100 is substantially rectangular, phone 500 has a curve shaped body, whereas phone 700 has a
20 multi-section body. The multi-section form factor includes a first section 716b and a second section 716c, and the second section 716c is further comprised of at least two sub-sections 716d-716e. The first and second sections 716b-716c may pivot towards each other as denoted by direction arrow 706a or away from each other opposite to the direction denoted by arrow 706a. Sub-section 716d
25 may rotate relative to sub-section 716e as denoted by the directions denoted by

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

arrows **706b**. In other words, phone **700** may be considered as an improved version of what is commonly referred to as "flip" phones.

Similar to the earlier described embodiments, phone **700** is provided with operating logic having a security function as earlier described, and power on/off button **722** with an integrated finger print reader. Except, power on/off button **722** with the integrated finger print reader is disposed at a front surface of lower section **716c** of phone **700** instead.

In alternate embodiments, second section **716c** may be a uni-section, i.e. it is not further sub-divided into to relatively pivotable sub-sections.

10

In yet other embodiments, the reference figure print image may be provided to the wireless mobile phone in a secure manner, e.g. read from an identity card, via an identity card reader additionally provided to the wireless mobile phone.

15

Figures 7a-7b illustrate one such embodiment. As illustrated in **Fig. 7b**, wireless mobile phone **100** is additionally endowed with an identity card reader **740**. Identity card reader **740** (optionally, assisted by a device driver additionally provided to supplement operating logic **240**) is equipped to retrieve the earlier described reference finger print image from identity card **742**.

20

Preferably, identity card **742** has a form factor that is difficult to forge, and its issuance is governed by a secured process. Resultantly, security for wireless mobile phone **100** is further enhanced.

25

For the embodiment, identity card **742** comprises a smart electronic card **744** (commonly referred to as a smart card) (see **Fig. 8a-8b**), and the reference finger print image is pre-stored in the embedded smart card **744**. Operating logic **240** (optionally, supplemented by a corresponding reader device driver) retrieves

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

the reference finger print image from embedded smart card 744, on detection of the presence of identity card 742.

In various embodiments, the reference finger print image may be further protected via encryption, requiring operating logic 240 to possess the proper
5 decryption key to recover the reference finger print image after retrieval.

In yet other embodiments, the reference finger print image may be further protected via an authentication protocol, requiring wireless mobile phone 100 to be equipped with the appropriate credential to authenticate itself to smart card 744, before being allowed by smart card 744 to access the pre-stored reference
10 finger print image in smart card 744.

In yet other embodiments, the reference finger print image may be imprinted on identity card 742, and identity card reader 720 is an optical reader.

In yet still other embodiments, the reference finger print image may be encoded via a magnetic strip disposed on a surface of identity card 742, and
15 identity card reader 720 is a magnetic code reader.

These are just a few examples, other equivalent encoding/storing and reading/retrieving techniques may also be employed instead.

Conclusion and Epilogue

20 Thus, it can be seen from the above descriptions, a novel wireless mobile phone that can afford protection against unauthorized access to user data and/or usage of the phone has been described.

While the present invention has been described in terms of the foregoing embodiments, those skilled in the art will recognize that the invention is not
25 limited to the embodiments described. The present invention can be practiced

Attorney Docket No: 109909-132415
IPG No: P053Z

Express Mail No:
EL692649056US

with modification and alteration within the spirit and scope of the appended claims.

In particular, the present invention may be practiced with the finger print reader (optical or otherwise) not being integrated with power on/off button, as
5 well as employing additional and/or other means to authenticate a user.

Thus, the description is to be regarded as illustrative instead of restrictive on the present invention.

Attorney's Docket No.: 109909-132415
 Inventor(s): Engstrom et al.
 For: A Wireless Mobile Phone With Authenticated Mode of Operation Including Finger
 Print Based Authentication
 Express Mail Label No. EL692649056US

Page 1 of 9
 Application No.: Not yet assigned
 Date of Deposit: March 28, 2003

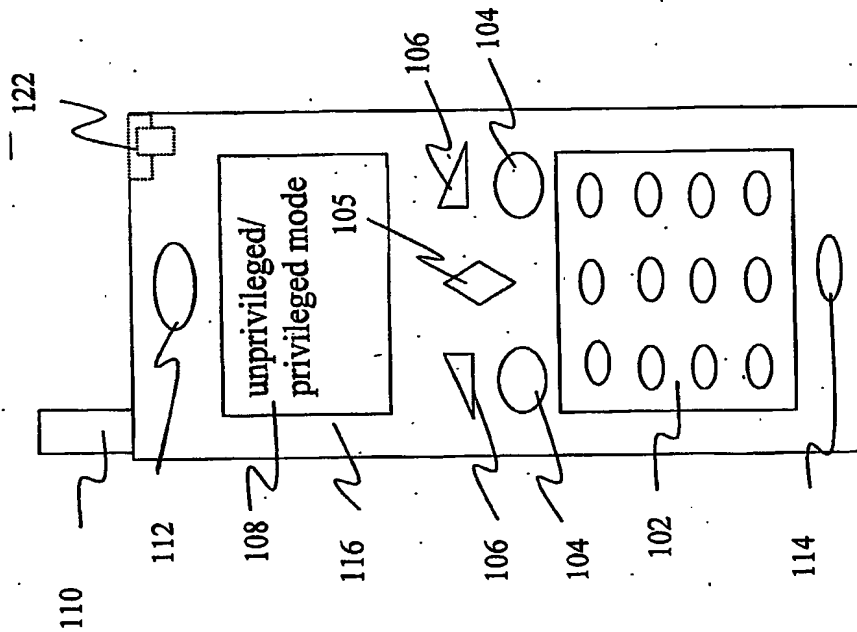


Figure 1

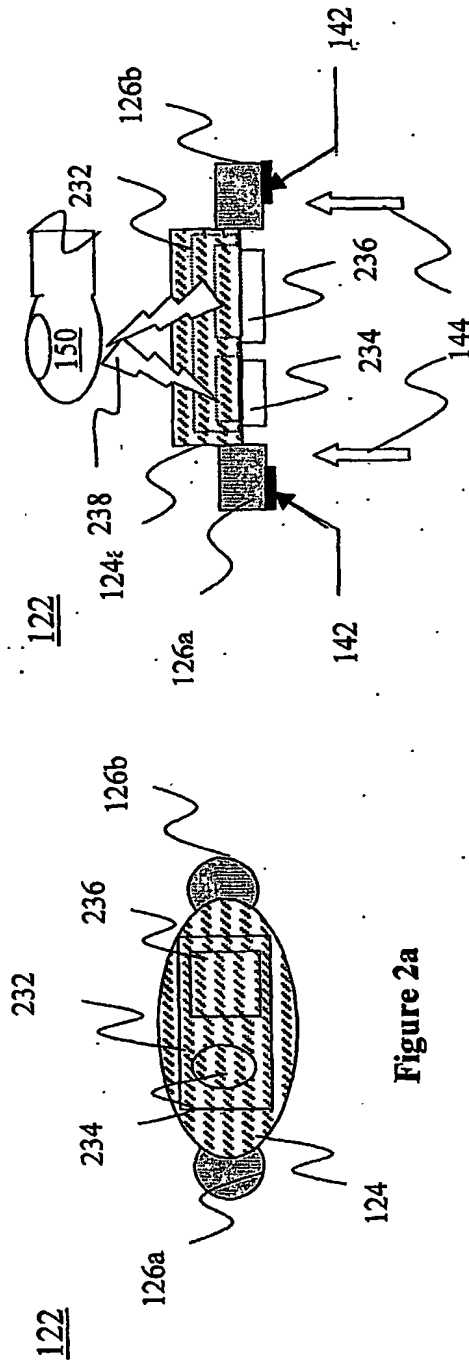


Figure 2b

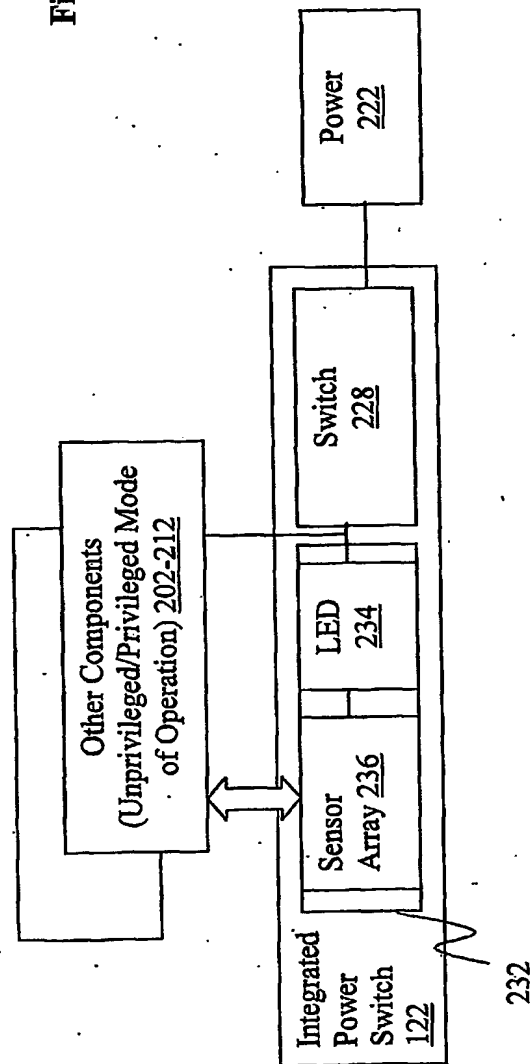


Figure 3a

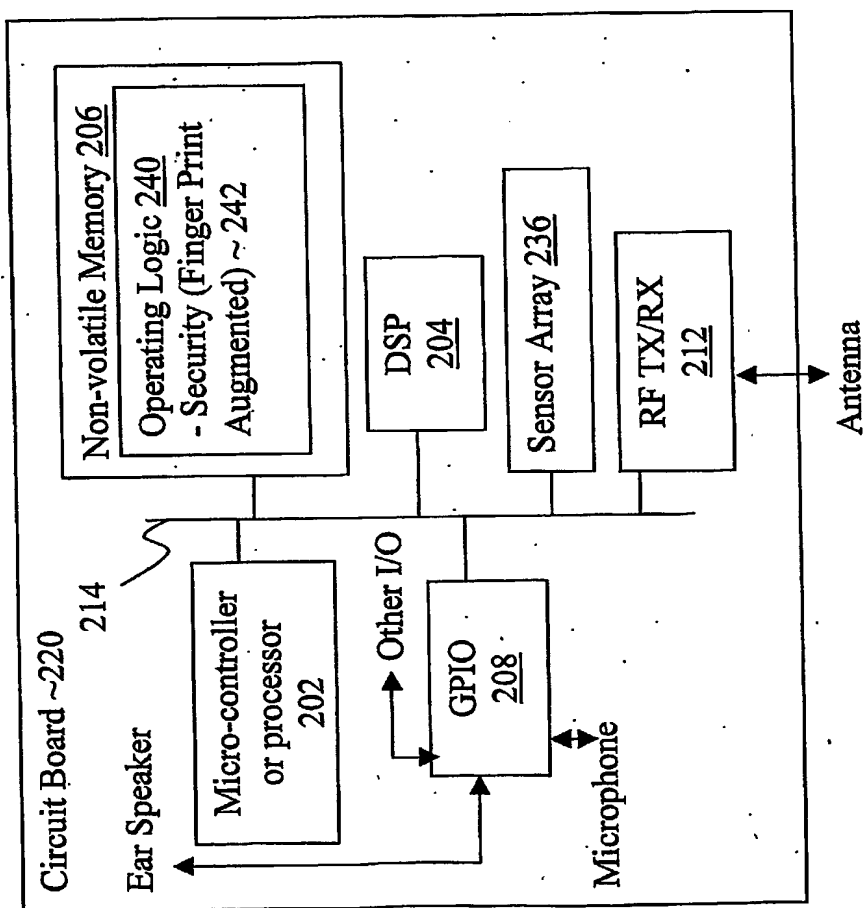


Figure 3b

Attorney's Docket No.: 109909-132415
 Inventor(s): Engstrom et al.
 For: A Wireless Mobile Phone With Authenticated Mode of Operation Including Finger
 Print Based Authentication
 Express Mail Label No. EL692649056US

Page 4 of 9
 Application No.: Not yet assigned
 Date of Deposit: March 28, 2003

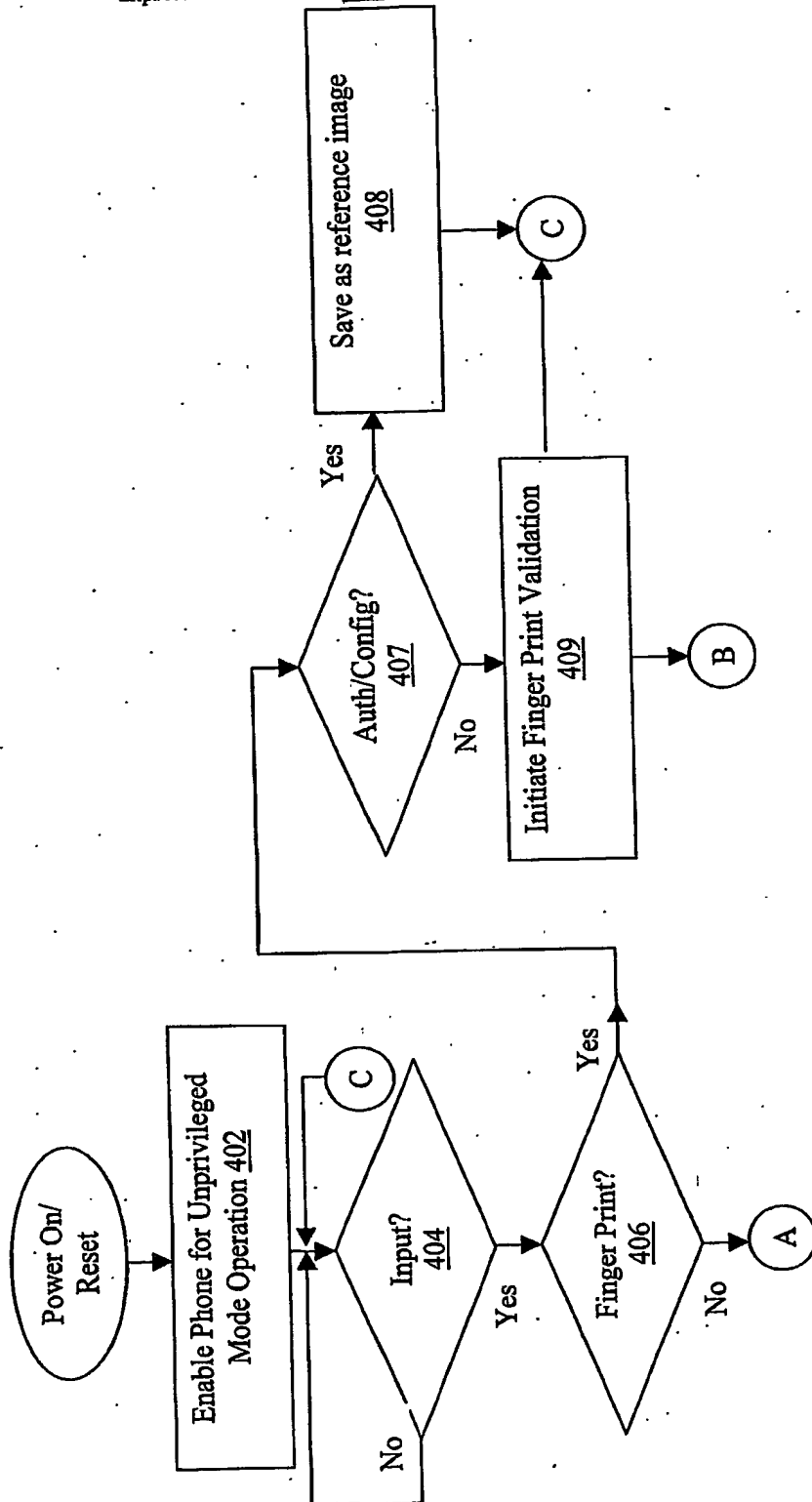


Figure 4a

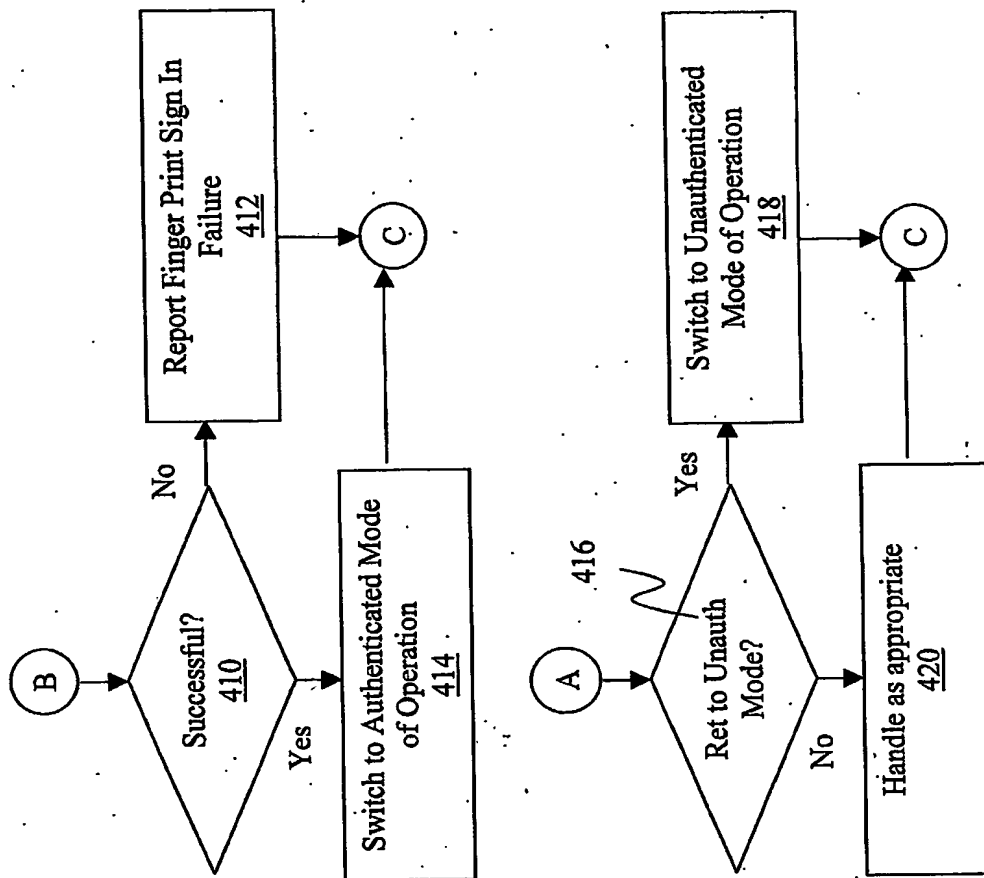


Figure 4b

Attorney's Docket No.: 109909-132415
Inventor(s): Engstrom et al.
For: A Wireless Mobile Phone With Authenticated Mode of Operation Including Finger
Print Based Authentication
Express Mail Label No. EL692649056US

Page 6 of 9
Application No.: Not yet assigned
Date of Deposit: March 28, 2003

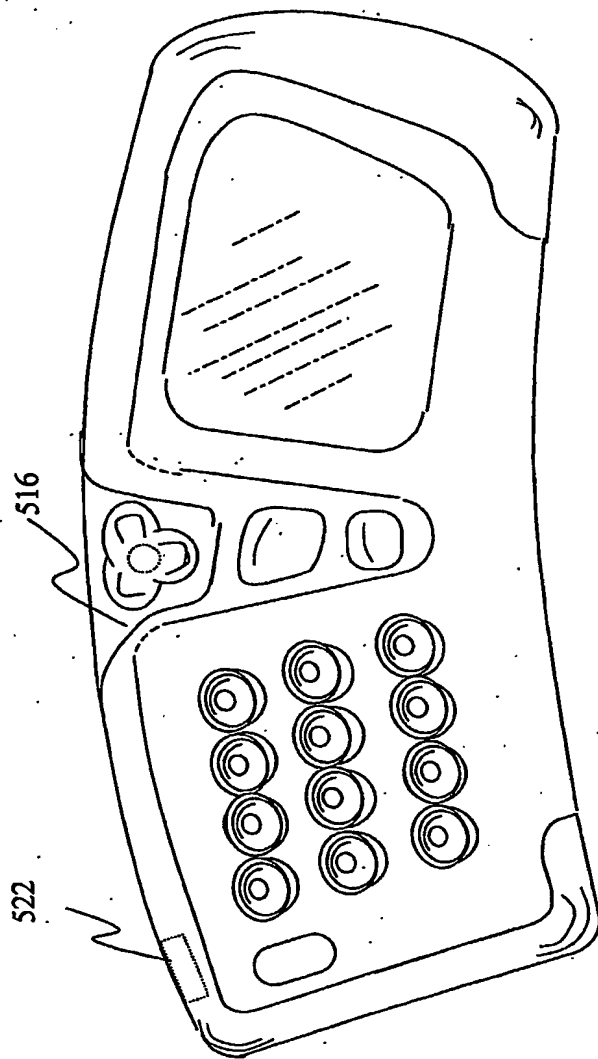
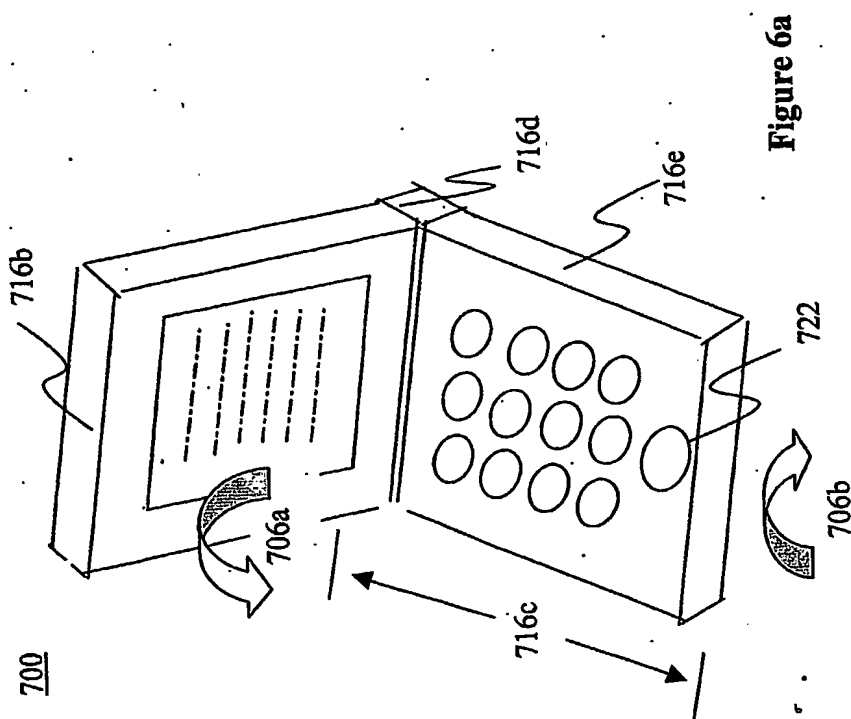
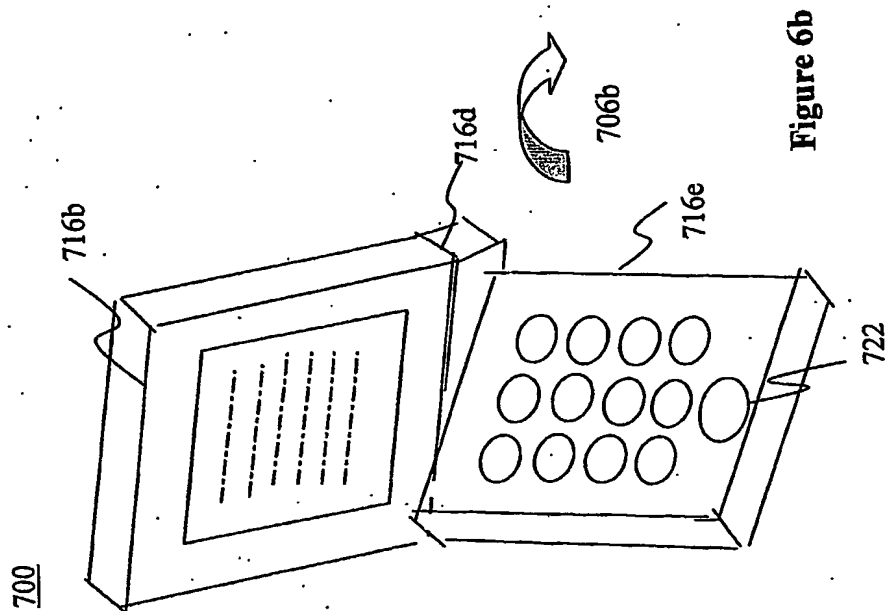


Figure 5

500



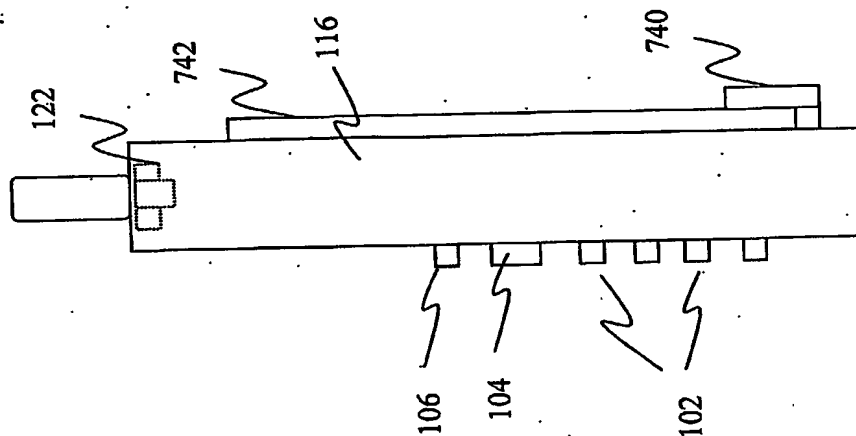


Figure 7b

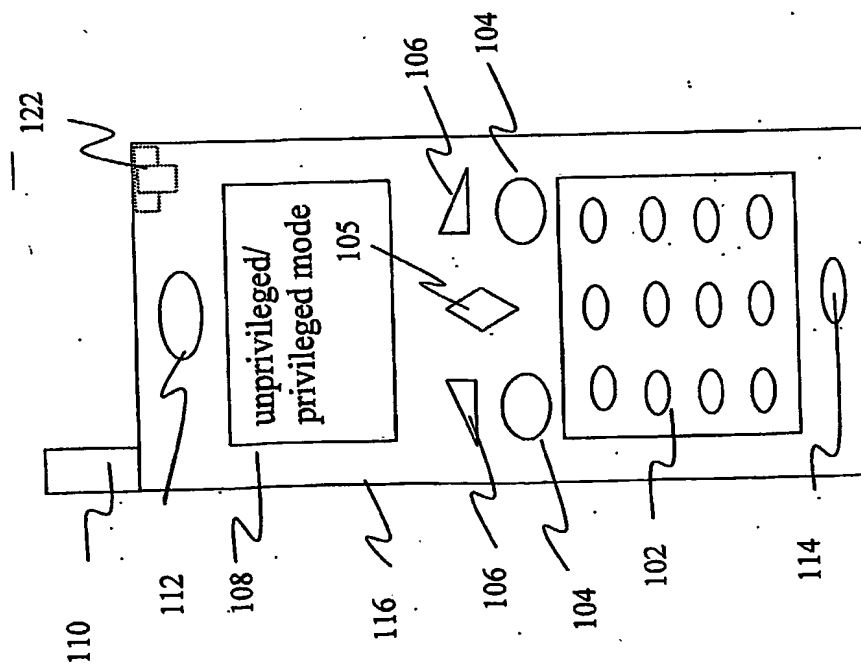


Figure 7a

Attorney's Docket No.: 109909-132415
Inventor(s): Engstrom et al.
For: A Wireless Mobile Phone With Authenticated Mode of Operation Including Finger
Print Based Authentication
Express Mail Label No. EL692649056US

Page 9 of 9
Application No.: Not yet assigned
Date of Deposit: March 28, 2003

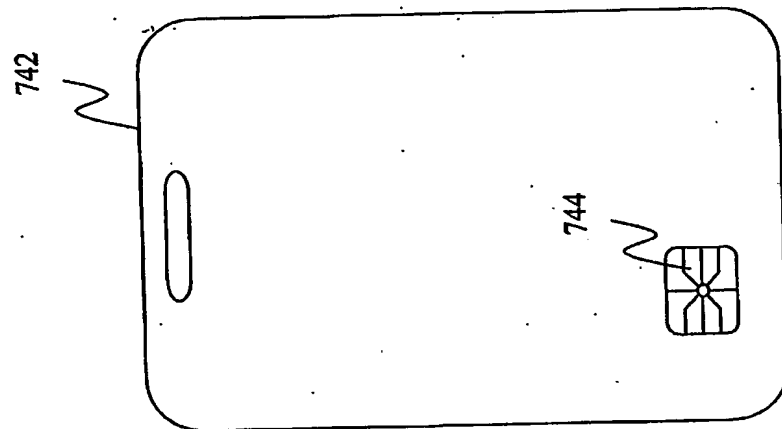


Figure 8b

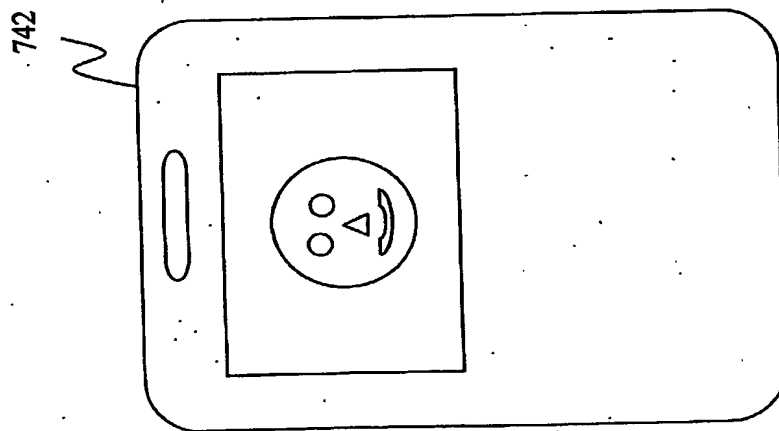


Figure 8a

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.